Security Groups

Section III (a)

Policies

(a) Participating agencies will be assigned Security Groups on an as-needed basis.

(b) System infrastructure equipment will reside in one or more Security Groups separate from user equipment. As configuration of the infrastructure is critical to the proper functioning of the system and has the potential to impact every user on the system, infrastructure Security Groups will be managed by IPSC.

(c) Application and security access rights for each agency will be approved by IPSC.

(d) Agencies should not attempt to manage another agency's resources, unless specifically authorized by that agency.

1) Background

"Security Groups" provide the framework for managing users and resources in the system. Each system resource, including user radios, talkgroups, dispatch consoles and radio sites, is assigned to a specific Security Group. System administrators are given access to items in a Security Group via a user account.

2) Capabilities

(a) There are an unlimited number of Security Groups and user accounts supported on the system.

(b) Security Groups are a "repository" for managing specific system resources, e.g., user radios, talkgroups, dispatch consoles and radio sites, in the system.

(c) User accounts permit administrators to manage the resources in their assigned Security Group. User accounts may be assigned any or all of the following rights for managing the items in a specific Security Group:

Access	Capabilities
Read	View the records of objects in the Security Group.
Insert	Add records to the Security Group.
Update	Update the information of objects in the Security Group.
Delete	Delete records from the Security Group.
Fault	Acknowledge and/or delete alerts and alarms and perform diagnostics for objects in the Security Group.
Grant	
Attach	
Regroup	Reassign users to a different talkgroup via the Dynamic Regrouping application.

(d) Each Administrator can be given access to any or all of the following applications:

i) Omnilink Zone Manager
ii) User Configuration Manager
iii) Radio Control Management
iv) SmartZone OmniLink System Reports
v) Air-Traffic-Statistics

(e) Agencies can share the same Security Group in order to minimize management complexity.

(f) The highest system user is the Super Manager, which has access to all resources on the system, regardless of which Security Group the resources reside in.

3) Constraints

(a) In order to manage users and talkgroups, and Administrator must have physical access to a SmartZone Manager workstation.

(b) Administrators with full access to a Security Group can disable any or all radios and talkgroups in that Security Group.

(c) Security Groups that contain a large number of records may be cumbersome and may require extensive search times to locate individual records.

(d) Once a Security Group is created, it cannot be deleted. However, the name of a Security Group can be changed.

(e) Security Group names must be from 1 to 12 alphanumeric characters.

(f) User Login Names must be from 1 to 8 lowercase alphanumeric characters.

4) Recommendations

(a) Grant each user the most restrictive access rights necessary in order to perform the desired task. Granting unlimited access to users increases the likelihood of accidental or unauthorized use.

(b) Specific training, expertise and hardware are required to effectively manage resources on the statewide system. Agencies are encouraged to work together to identify the necessary resources to manage their users on a regional basis.

(c) In some cases, IPSC staff may be able to provide management capabilities for smaller agencies. This can be discussed on a case-by-case basis.